POLYNOMIAL METHODS: RECENT ADVANCEMENTS IN COMBINATORICS

by

Thomas Fleming

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

Major: Mathematical Sciences

The University of Memphis

December 2021

ACKNOWLEDGMENTS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

ABSTRACT

Fleming, Thomas Rexford. M.Sc. The University of Memphis. May 2021. Polynomial Methods: Recent Advancements in Combinatorics. Major Professor: Dr. David Grynkiewicz.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

TABLE OF CONTENTS

Contents **Pages**

Chapter 1

Introduction and Preliminary Results

1.1 Introduction

One of the earliest objects of algebraic study, real (specifically integral) univariate polynomials generalize the most simple algebraic objects, linear functions, and have significant application. Beyond this, multivariate polynomials offer further generalization. Expanding even further, multivariate polynomials over arbitrary rings (and fields) prove surprisingly useful. In this thesis, we will showcase a variety of methods and applications involving polynomials. These applications will prove some surprising results, both abstract and concrete. To understand these proofs, one need only thorough knowledge of algebraic tools and structures, and some experience with methods of combinatorial proof.

Merging the fields of Combinatorics and Number Theory yields Combinatorial Number Theory and Additive Combinatorics, two overlapping fields answering questions pertaining to zero-sums over sequences and zeroes of arbitrary polynomials as well as other problems at the intersection of Combinatorics, Algebra, and Number Theory. We begin Chapter 1 by presenting many common objects which we will make use of throughout the thesis. This will include some objects of common study, such as polynomials, as well as some notation and conventions common to the field, and the statements of a few common theorems which the reader will likely be familiar with. After this, in chapter 2, we introduce the Nullstellensatz, literally translating as zero-locus theorems, a series of theorems concerning the number of common zeroes of a family of polynomials. These theorems, while extremely powerful, will have relatively simple statements and proofs culminating in the Punctured Nullstellensatz. Moving on, in chapter 3 we demonstrate some applications of these Nullstellensatz. These will mostly make use of the simplest version of the Nullstellensatz which we present, Alon's Combinatorial Nullstellensatz II [1]. The applications will come in two main varieties, sumset proofs and

graph theoretic proofs. This chapter will provide some of the most concrete applications of the polynomial method. In chapter 4 we present Dyson's theorem [6] on laurent polynomials and Zeilberger and Bressoud's q-Dyson variant, with a proof based on a concrete version of the Combinatorial Nullstellensatz [5]. In chapter 5 we provide Reiher's proof of the Kemnitz conjecture [7], on the minimal size of a set of ordered pairs required to have a subset of size p whose elements are zero-sum over the finite field F_p. This proof will make heavy use of the theorem of Chevalley and Warning, our other major trick in the bag of polynomial methods concerning zero-sum methods. In chapters 6 and 7 we prove some longer results from additive combinatorics concerning zero-sum sequences, and in chapter 8 we provide a few nontrivial applications of these methods in other areas. Overall, we aim to provide a wide breadth of results demonstrating the power of these polynomial methods in a diverse range of fields. First, though, in chapter 2 we will provide proofs of these results which will prove so powerful in later sections.

1.2 Definitions, Notation, and Preliminary Results

Before we continue on, we define a few basic objects and results in use throughout the thesis. Readers are assumed to have knowledge equivalent to a first course in group and ring theory and a first course in combinatorics.

Definition 1.1 (Polynomial Ring)**.** Given a ring R, we define $R[x]$ to be the ring generated by all formal sums of the form $f = \sum_{i=0}^{\infty} c_i x^i$, $c_i \in R$ where there is a $N \in \mathbb{N}_0$ so that $c_i = 0$ for all $i \geq N$ with ring operations given by the standard componentwise formulae. We call $R[x]$ **the polynomial ring** in 1 variable over R.

Definition 1.2 (Multivariate Polynomial Ring)**.** Given a ring R, we define a **polynomial ring** over n variables, $R[x_1, \ldots, x_n]$ inductively by the rules $R[x_1] = R[x]$ and $R[x_1, \ldots, x_i] = (R[x_1, \ldots, x_{i-1}])[x_i]$.

Definition 1.3 (Laurent Polynomial)**.** Given a field F, we define a **laurent polynomial ring** in n variables over F as $F\left[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\right]$.

Definition 1.4 (Monomial)**.** Given a ring R, a polynomial $f \in R[x_1, \ldots, x_n]$ is a monomial if $f = \prod_{i \in J} x_i$ where $J \subseteq \{1, \ldots, n\}$.

Definition 1.5 (Degree)**.** We define the **degree** of a polynomial $f \in R[x]$ as

$$\deg(f) = \min\{N \in \mathbb{N}_0 : c_i = 0 \,\forall\, i \geq N\}.$$

By convention the zero polynomial has degree -1. For multivariate polynomial rings there are two natural generalizations of degree, total degree and projected degree. For a polynomial

$$f = \sum_{i_1,\ldots,i_n \in N_0} c_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n} \in R[x_1, \ldots, x_n]$$

we define the **total degree** as

$$\deg(f) = \min\{N \in N_0 : c_{i_1,\ldots,i_n} = 0 \,\forall\, i_1, \ldots, i_n \in N_0 \text{ so that } \sum_{j=1}^{n} i_j \leq N\}$$

and we define the **projected degree in variable** x_k by letting

$$J = (R[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n])[x_k]$$

which one can readily verify is the same as $R[x_1, \ldots, x_n]$. Then,

$$\deg_{x_k}(f) = \deg_J(f)$$

where $\deg_J(f)$ is simply the degree over the given ring J.

Definition 1.6 (Module)**.** Given a ring R, we define a (left) R-module M to be a set endowed with two operations, addition and multiplication, such that $+ : M \times M \to M$ and $\cdot : R \times M \to M$ with $+$ satisfying the axioms of an abelian group and $\cdot$ being associative, having an identity, and having both left and right distributive laws ($(r+s)\,x = rx + sx$ and $r\,(x+y) = rx + ry$ for $r, s \in R$ and $x, y \in M$). If R is a module, we instead call M a vector space.

In a vector space M, we call the set $x_1, \ldots, x_n$ a basis of M if is linearly independent and spans M.

Definition 1.7 (Zero-Sum)**.** Given $n, p \in \mathbb{N}$ and a subset $I \subseteq \mathbb{Z}^n$, we say a I is zero-sum if $\sum I = \sum_{i \in I} i \equiv 0 \mod p$.

Definition 1.8 (Characteristic Function)**.** Given a vector $\mathbf{x}$, the characteristic function $\chi_{\mathbf{x}}$ has $\chi_{\mathbf{x}}(\mathbf{y}) = \begin{cases} 1, & \mathbf{x} = \mathbf{y} \\ 0, & \mathbf{x} \neq \mathbf{y} \end{cases}$

Definition 1.9 (Map Functor)**.** For a field F and $m \geq 0$, define $\mathrm{Map}\left(\{0,1\}^m, F\right) = \{f : \{0,1\}^m \to F | f \text{ is a function}\}$.

Notation (Polynomial Coefficient)**.** For a laurent polynomial

$$f = \sum_{i_1, \ldots, i_n \in \mathbb{Z}} c_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n}$$

over n variables, we denote the coefficient of a particular term by $\left[x_1^{i_1} \ldots x_n^{i_n}\right] f \coloneqq c_{i_1, \ldots, i_n}$ when it is more convenient.

Notation (Vector Polynomials)**.** For a laurent polynomial $f(x_1, \ldots, x_n)$ evaluated at

$x_1, \ldots, x_n$, we implicitly denote $\mathbf{x} = (x_1, \ldots, x_n)$ and $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ when it is unambiguous and convenient.

Notation (Congruence)**.** For a congruence statement $a \equiv b \pmod{c}$ we sometimes shorten it to $a \equiv b$ when the modulus c is unambiguous.

Notation (Integer subsets)**.** Given an upper bound p, we denote the set of all natural numbers less than or equal to p by $[1, p] = \{x \in \mathbb{Z} : 1 \leq x \leq p\}$. In general, $[q, p] = \{x \in \mathbb{Z} : q \leq x \leq p\}$. This notation will only be used when it is unambiguous with the normal notation for closed intervals.

Notation (Sum over set)**.** For a set A on which a sum is well defined, we define $\sum A = \sum_{a \in A} a$ where it is unambiguous. Similarly, $\sum_A f(a) = \sum_{a \in A} f(a)$.

The next theorem has many equivalent statements as well as a few stronger (and weaker) ones. For the rest of this thesis, we will assume the Fundamental Theorem of Algebra refers to the following statement.

Theorem 1.1 (Fundamental Theorem of Algebra)**.** Given a ring R and $f \in R[x]$ with $\deg(f) = n \geq 0$, let $X = \{x \in R : f(x) = 0\}$. Then, $|X| \leq n$.

Chapter 2

Nullstellensatz

2.1 Hilbert's Nullstellensatz

Before we can approach the Combinatorial Nullstellensatz, or any other tools of the polynomial method, it is important to see a closely related theorem, Hilbert's Nullstellensatz. This theorem is more algebraic in nature, though its influence in the Combinatorial Nullstellensatz will be clear. One statement of this theorem is as follows,

Theorem 2.1 (Hilbert's Nullstellensatz [1])**.** Let F be an algebraically closed field and $f, g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$. If for all common zeroes of $g_1, \ldots, g_m$ we find f to be zero, then there is an integer k and polynomials $h_1, \ldots, h_m \in F[x_1, \ldots, x_m]$ such that $f^k = \sum_{i=1}^{n} h_i g_i$.

For a proof of this see

Cite good proof of Hilbert's Null-stel-lensatz

This theorem, though closely related to the Combinatorial Nullstellensatz, will see no use in this thesis, though their historical and mathematical relation are good to keep in mind. With this, we now introduce the main theorem of this thesis, Alon's Combinatorial Nullstellensatz.

2.2 Alon's Combinatorial Nullstellensatz

Alon's theorem is actually a special case of Hilbert's, that is when $n = m$ and each g_i is univariate and of the form $\prod_{s \in S_i} (x_i - s)$. These extra conditions allow a stronger conclusion to be drawn, namely that f can split into polynomials of lesser collective degree than itself. Though this statement is non-rigorous, it is immediately clear that turning one polynomial into a sum of simpler polynomials can have useful corollaries. It is in fact one of these corollaries that we will make use of throughout the rest of this thesis. Before we can prove such a theorem, though, we need to state and prove the following lemma:

Lemma 2.1. [1] Let R be an integral domain and $n \geq 1$, $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$, and $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty.

Suppose $\deg_{x_i} f < |A_i|$ for each $1 \leq i \leq n$ and $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Then f is the zero polynomial.

Proof. Let F be the quotient field of R. Clearly, any polynomial in R is a polynomial in F and as $f = 0$ in F implies $f = 0$ in R we need only consider the case $F = R$. We will proceed by induction on n. We already know the case $n = 1$ holds by the Fundamental Theorem of Algebra (or a corollary thereof). Now, we prove the case n. First, let us define $f_i(x_1, x_2, \ldots, x_{n-1})$ to be the non x_n component of f, that is

$$f(\mathbf{x}) = \sum_{i=0}^{\deg_{x_n} f} f_i(x_1, x_2, \ldots, x_{n-1})\, x_n^i.$$

We see each $f_i \in F[x_1, x_2, \ldots, x_{n-1}]$ and $\deg_{x_j} f_i \leq \deg_{x_j} f < |A_i|$ for all $1 \leq j \leq n-1$ and $0 \leq i \leq \deg_{x_n} f$. Let $a_i \in A_i$ be an arbitrary element for each $0 \leq i \leq n-1$. As $f(a_1, a_2, \ldots, a_{n-1}, a) = 0$ for all $a \in A_n$ and $\deg_{x_n} f < |A_n|$, the $n = 1$ case implies that $f(a_1, a_2, \ldots, a_{n-1}, x_n) = 0$ must be the zero polynomial. Hence $f_i(a_1, \ldots, a_{n-1}) = 0$ for

each $1 \leq i \leq n$ and each $(a_1, \ldots, a_{n-1}) \in \prod_{i=1}^{n-1} A_i$. Hence, by the inductive hypothesis each f_i is the zero polynomial, so f is the zero polynomial. $\square$

This lemma comprises the majority of the intellectual heavy lifting for our main theorem, and thus its proof will appear very simple in comparison to its powerful statement:

Theorem 2.1 (Generalized Combinatorial Nullstellensatz [4])**.** Let R be an integral domain, $n \geq 1$, and let $A_1, A_2, \ldots, A_n \subseteq R$ be finite and nonempty.
Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and define $g_i(x_i) = \prod_{a \in A_i} (x_i - a)$ for $1 \leq i \leq n$. Then, $f(a_1, a_2, \ldots, a_n) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ if and only if there are polynomials $h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ such that

- $f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) \Big(h_i(\mathbf{x}) \Big)$,
- $\deg(g_i) + \deg(h_i) \leq \deg(f)$ for $1 \leq i \leq n$,
- $\deg_{x_j}(g_i) + \deg_{x_j}(h_i) \leq \deg_{x_j}(f_i)$ for all $1 \leq i, j \leq n$.

Proof. First, suppose $A_1, A_2, \ldots, A_n \subseteq R$ and $f(\mathbf{x}) \in R[x_1, \ldots, x_n]$. Let, $g_i = \prod_{a \in A_i} (x_i - a)$. Then, examining the backwards implication, it is clear that $f(\mathbf{a}) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$. Now, let us examine the forwards implication . First, let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial which is zero on all of $A_1 \times A_2 \times \ldots \times A_n$. We wish to show that the polynomials h_i exists for each i, such that each h_i satisfies the conditions of the theorems. For each $1 \leq j \leq n$ define g_{ji} as follows:

$$g_j(x_j) = \prod_{a \in A_j} (x_j - a) = x_j^{|A_j|} - \sum_{i=0}^{|A_j|-1} g_{ji} x_j^i, \tag{2.1}$$

where each $g_{ji} \in R$ as well. Hence, as $a_j \in A_j$ implies that $g_j(a_j) = 0$ we must have that $a_j^{|A_j|} = \sum_{i=0}^{|A_j|-1} g_{ij} a_j^i$. Now, we define a new polynomial $\overline{f}$, such that $\overline{f}$ is f after a repeated application of the substitution $x_j^{|A_j|} \to \sum_{i=0}^{|A_j|-1} g_{ij} x_j^i$. We see that

$\deg_{x_i}\left(\overline{f}\right) < |A_i|$ for each i(as any monomial term of such degree can be substituted for terms of lesser degree), and as $\overline{f}\left(\mathbf{a}\right) = f\left(\mathbf{a}\right) = 0$ for each $\mathbf{a} \in \prod_{i=1}^{n} A_i$ (This fact is trivial by the construction of f and $\overline{f}$), then by the preceding lemma we have that $\overline{f} = 0$. Next, consider the polynomial $f\left(\mathbf{x}\right) - \overline{f}\left(\mathbf{x}\right)$. Define $f_0 = f$ and f_i to be f after the i'th such substitution. Furthermore, let $N \in \mathbb{N}$ be such that $f_N = \overline{f}$. Then, the polynomial f_i is obtained by examining a term of f_{i-1} with a degree in x_j of at least $|A_j|$ and replacing an individual factor of $x_j^{|A_j|}$ by the sum as we defined earlier. For simplicity let us take the term $cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} \cdot x_j^{|A_j|}$ (where $k_j \geq 0$ by our construction) and apply such a substitution. Then, we see that the difference

$$f_{i-1} - f_i = cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\left(x_j^{|A_j|} - \sum_{i=0}^{|A_j|-1} g_{ji}x_j^i\right) = cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} \cdot g_j\left(x_j\right)$$

by 2.1. Furthermore, as $f_N = \overline{f}$ we have that

$$f - \overline{f} = \left(f_0 - f_1\right) + \left(f_1 - f_2\right) + \ldots + \left(f_{N-1} - f_N\right).$$

Hence, $f = f - 0 = f - \overline{f} = \sum_{j=1}^{n} g_j\left(x_j\right) h_j$ where each $h_j \in R[x_1, x_2, \ldots, x_n]$ is simply the sum of all of these preceding terms $cx_1^{k_1}\ldots x_n^{k_n}$ as a result of these substitutions. Furthermore, we had by construction that $\deg g_j = |A_j| > \deg\left(\sum_{i=0}^{|A_j|-1} g_{ji}x_j^i\right)$, so we see that such a substitution will never increase the degree of our polynomial and hence $\deg f_i \leq \deg f$. Then, as $\deg g_j = |A_j|$, we see that

$$\deg\left(cx_1^{k_1}\ldots x_n^{k_n}g_j(x_j)\right) \leq \deg f_{i-1} \leq \deg f.$$

Using the additive nature of polynomial degree yields $\deg\left(cx_1^{k_1}\ldots x_n^{k_n}\right) + \deg g_j \leq \deg f$, and as each h_j is simply the sum of such terms we may substitute its degree to yield $\deg g_j + \deg h_j \leq \deg f$.

Lastly, we show this holds for projected degree as well. Note that as we are replacing a term g_j with $\deg_{x_k}(g_j) = 0$, and as each h_j with $\sum_{i=0}^{|A_j|-1} g_{ji}x_j^i$ also has projected degree 0, the overall degree in x_k will not change after i substitutions. Hence for $k \neq j$, $\deg_{x_k}\left(cx_1^{k_1}\dots x_n k_n g_j(x_j)\right) = \deg_{x_k}(f_{i-1}) = \deg_{x_k}(f)$. Moreover, if $k = j$, the same argument shows the projected degrees decrease. These facts yield $\deg_{x_k}\left(cx_1^{k_1}\dots x_n^{k_n}\right) + \deg_{x_k}(g_j) = \deg_{x_k}(f)$. And, as each h_j is simply the sum of these remaining terms, we see $\deg_{x_k}(h_j) + \deg_{x_k}(g_j) \leq \deg_{x_k}(f)$ for each $1 \leq j, k \leq n$. □

This theorem is perhaps too general and too powerful for use in proving our simpler results. As a corollary, many authors include a weaker second statement of the theorem, where the splitting of a polynomial is replaced by a constraint on the cardinality of the set on which $f(\mathbf{x}) = 0$.

Theorem 2.2 (Combinatorial Nullstellensatz [4])**.** Let R be an integral domain, $n \geq 1$, and $A_1, A_2, \dots, A_n \subseteq R$ be finite and nonempty, with $f(\mathbf{x}) \in R[x_1, x_2, \dots, x_n]$ being a polynomial. Suppose

$$[x_1^{d_1}x_2^{d_2}\dots x_n^{d_n}]f(\mathbf{x}) \neq 0$$

and that $\deg f = \sum_{i=1}^{n} d_i$ with $0 \leq d_i \leq |A_i| - 1$. Then, there exists an element $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. That is, given a nontrivial "maximal degree" monomial of f such that the degree of this monomial in each variable, x_i, is strictly less than the size of the corresponding set A_i, f cannot be zero on the whole of the product of the A_i.

This is in essence a generalization of the Fundamental theorem of Algebra and it is precisely this simple statement about the number of zeroes of a particular polynomial which provides our combinatorial power. The proof follows rather directly from the generalized version as follows:

Proof. Let $g_i = \prod_{a \in A_i}(x_i - a)$ for $1 \leq i \leq n$ and suppose the contrary. That is,

$f(\mathbf{a}) = 0$ for all $\mathbf{a} \in \prod_{i=1}^{n} A_i$ despite the assumptions of the construction. Then, the generalized combinatorial nullstellensatz yields polynomials with the desired properties, which we will denote as $h_1, h_2, \ldots, h_n \in R[x_1, x_2, \ldots, x_n]$. Now let us examine the nature of $[x_1^{d_1} \ldots x_n^{d_n}] f(\mathbf{x})$. As this is a maximal degree monomial of f, then only maximal degree monomials of $h_i(\mathbf{x}) g_i(x_i)$ can contribute to its coefficient in f as $\deg(h_i) + \deg(g_i) = \deg h_i g_i \leq \deg f$. However, by the construction of g_i, all such monomials will be taken from the $h_i(\mathbf{x}) \cdot x_i^{|A_i|}$ portion of this polynomial. Thus $\deg_{x_i} h_i g_i > d_i$ by our requirement that each $d_i < |A_i|$, hence all maximal degree monomials of f must be of the form $x_1^{k_1} x_2^{k_2} \ldots x_j^{|A_j|} \ldots x_n^{k_n}$. Thus, we must have $[x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}] f(\mathbf{x}) = 0$, $\lightning$. Hence, there must be some $\mathbf{a} \in \prod_{i=1}^{n} A_i$ such that $f(\mathbf{a}) \neq 0$. □

Our last version of the Combinatorial Nullstellensatz will examine what happens when f vanishes over not all, but most (in a certain set-theoretic perspective) of the members of the product. This is known as the Punctured Combinatorial Nullstellensatz and it builds on the original generalized version. The proof will involve division of polynomials of many variables, so let us first examine the nature of such an operation.

2.3 Ball and Serra's Punctured Nullstellensatz

Sometimes we will not have polynomials which are zero over the whole of a set, but just on part. These conditions yield the Punctured Nullstellensatz. But, before we may state the theorem itself, we must state a result about the well-behavedness of multivariate polynomial division.

Lemma 2.1 (Multivariate Polynomial Division)**.** Let R be an integral domain and let $g_1(x_1), \ldots, g_k(x_k) \in R[x_1, x_2, \ldots, x_n]$ be polynomials of one variable with leading coefficient 1 for $1 \leq k \leq n$. Then,

1. If $f \in \sum_{i=1}^{k} R[x_1, \ldots, x_n] \cdot g_i(x_i)$ is a nonzero polynomial in the ideal generated by $g_1(x_1), \ldots, g_k(x_k)$ over $R[x_1, \ldots, x_n]$, then $\deg_{x_i}(f) \geq \deg(g_i)$ for some $1 \leq i \leq k$.

2. For a polynomial $f \in R[x_1, \ldots, x_n]$ there are $w(\mathbf{x}), h_1(\mathbf{x}), \ldots, h_k(\mathbf{x}) \in R[x_1, \ldots, x_n]$ such that all of the following hold :

   - $f(\mathbf{x}) = \sum_{i=1}^{k} h_i(\mathbf{x}) g_i(x_i) + w(\mathbf{x})$.
   - $\deg_{x_j}(w) < \deg(g_j)$ for $1 \leq j \leq k$,
   - $\deg_{x_j}(g_i) + \deg_{x_j}(h_i) \leq \deg_{x_j}(f)$ for $1 \leq i \leq k$, $1 \leq j \leq n$,
   - $\deg(g_i) + \deg(h_i) \leq \deg(f)$ for $1 \leq i \leq k$,
   - $\deg_{x_i}(w) \leq \deg_{x_i}(f)$ for $1 \leq i \leq n$,
   - $\deg(w) \leq \deg(f)$.

Furthermore, the polynomial $w(\mathbf{x})$ is unique .

As this proof is rather lengthy and unrelated to the topic at hand, we omit it. For a rigorous proof see [4]. With these constraints now understood, we state and prove the Punctured Nullstellensatz.

Theorem 2.1 (Punctured Combinatorial Nullstellensatz [4])**.** Let R be an integral domain and let $A_1, A_2, \ldots, A_n \subset R$ be finite and nonempty. Furthermore, for each $1 \leq i \leq n$ let $B_i \subseteq A_i$ be nonempty.

Let $f(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$ be a polynomial and set $g_i(x_i) = \prod_{a \in A_i}(x_i - a)$ and $l_i(x_i) = \prod_{b \in B_i}(x_i - b)$. If

$$f(\mathbf{a}) = 0 \; \forall \; \mathbf{a} \in \left(\prod_{i=1}^{n} A_i\right) \setminus \left(\prod_{i=1}^{n} B_i\right) \tag{2.2}$$

but there exists a $\mathbf{b} \in \prod_{i=1}^{n} B_i$ such that $f(\mathbf{b}) \neq 0$ then there are polynomial $h_i \in R[x_1, x_2, \ldots, x_n]$ with $1 \leq i \leq n$ such that

$$f(\mathbf{x}) = \sum_{i=1}^{n} g_i(x_i) h_i(\mathbf{x}) + w(\mathbf{x}) \text{ with } w(\mathbf{x}) = u(\mathbf{x}) \prod_{i=1}^{n} \frac{g_i(x_i)}{l_i(x_i)}.$$

with the following conditions holding:

$\deg(w) \leq \deg(f) \deg_{x_j}(w) \leq \deg_{x_j}(f)$ for all $1 \leq j \leq n$, $\deg_{x_i}(w) < |A_i|$,

$\deg(g_i) + \deg(h_i) \leq \deg(f)$ for $1 \leq i \leq n$ and

$\deg_{x_j}(g_i(x_i)) + \deg_{x_j}(h_i) \leq \deg_{x_j}(f)$ for $1 \leq i, j \leq n$. Consequently $\sum_{i=1}^{n}(|A_i| - |B_i|) \leq \deg(w) \leq \deg(f)$.

Proof. The preceding lemma guarantees there to be polynomials

$$w(\mathbf{x}), h_1(\mathbf{x}), \ldots, h_n(\mathbf{x}) \in R[x_1, x_2, \ldots, x_n]$$

of the desired form and for which the proper conditions hold (case 2). Our task, then, is to ensure that the form of $w(\mathbf{x})$ is that of our statement. First, let $1 \leq i \leq n$ and without loss of generality select $i = 1$. First, we consider $w(\mathbf{x}) l_1(x_1)$. Then as f and the first sum of equation (2) must be zero on all $\mathbf{a} \in \prod_{i=1}^{n} A_i \setminus \prod_{i=1}^{n} B_i$, we see $w(\mathbf{x})$ must also vanish on this difference of products. Furthermore, by the construction of l_1 we must have that

$w(\mathbf{x})\, l_1(x_1)$ vanishes on $\prod_{i=1}^{n} B_i$ as well, hence it vanishes on all of $\prod_{i=1}^{n} A_i$. Applying theorem 1 (Generalized Combinatorial Nullstellensatz) yields polynomials $v_1, \ldots, v_n \in R[x_1, \ldots, x_n]$ such that

$$w(\mathbf{x})\, l_1(x_1) = \sum_{i=1}^{n} g_i(x_i)\, v_i(\mathbf{x}). \tag{2.3}$$

Now, by the preceding lemma we may assume that $v_j(\mathbf{x})$ is not of the form in case 1. Furthermore, for $n > 1$, we see $\deg_{x_n}(w(\mathbf{x})\, l_i(x_i)) > |A_n|$ as a consequence of the stipulations of $w(\mathbf{x})$. Now, for a polynomial $h \in f[x_1, ..., x_n]$ define $\overline{h}$ to be h reduced modulo the ideal generated by $g_1(x_1), \ldots, g_{n-1}(x_{n-1})$. Applying this operation to equation (4) yields

$$\overline{w(\mathbf{x})\, l_1(x_1)} = \overline{g_n(x_n)\, v_n(\mathbf{x})}.$$

□

Finish Proof of Punctured Nullstellensatz

With all three variations of the Combinatorial Nullstellensatz fully stated and proven, allow us to move on to the examination of some of the most powerful results which these theorems prove, namely in combinatorics. We will begin with a proof of the Chevalley-Warning theorem as well as several results of additive combinatorics concerning sumsets, both standard and restricted.

Maybe change proof to the one found in Simeon and Ball

Chapter 3

Simple Combinatorial Proofs

3.1 Sumsets

prove 1-2 more combinatorial statements with Nullstellensatz

Now, with our the Nullstellensatz stated and proven, let us examine a few simple results concerning sumsets, those being the pointwise sum of all coordinates

Theorem 3.1 (Cauchy-Davenport Theorem [1])**.** Given a prime p and nonempty $A, B \subseteq Z_p$, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.

Proof. Suppose $|A|+|B| > p$, we must have that for any element $x \in Z_p$, $(A) \cap (x \setminus B) \neq \varnothing$ (As there are only p possible elements which could be in each set). Hence, $A+B = Z_p$. Thus, let us assume $|A|+|B| \leq p$ and suppose indirectly that $|A+B| \leq |A|+|B|-2$. Let $A+B \subseteq C \subseteq Z_p$ such that $|C| = |A|+|B|-2$. Next, define $f(x,y) = \prod_{c \in C}(x+y-c)$ and note that we must have $f(a,b) = 0$ for all $(a,b) \in A \times B$ as $A, B \subseteq C$. Now, note that $\deg(f) = |C| = |A|+|B|-2$, and hence $[x^{|A|-1}y^{|B|-1}]f(x,y) = \binom{|A|+|B|-2}{|A|-1} \neq 0$ as $|A|-1 < |A|+|B|-2 < p$. Hence, by the Combinatorial Nullstellensatz (Theorem 1.2), we must have a pair $(a,b) \in A \times B$ such that $f(a,b) \neq 0$ ↯. Thus, the theorem must be true. □

With this basic theorem about sumsets proven, we now take a look at restricted sumsets, those being sumsets where a sum is excluded if it satisfies a certain property, normally being the root of a particular polynomial.

Notation (Restricted Sumset)**.** For a polynomial $h(x_0, x_1, \ldots, x_k)$ and subsets $A_0, A_1, \ldots, A_k \subseteq Z_p$ define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + a_1 + \ldots + a_k : a_i \in A_i, h(a_0, a_1, \ldots, a_k) \neq 0\}$$

to be the restricted sumset over the A_is with respect to h.

Theorem 3.2 (General Restricted Sumset Theorem[1])**.** For a prime p and a polynomial $h(x_0, .., x_k)$ over Z_p and nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$, define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \deg(h)$.
If $[x_0^{c_0} \ldots x_k^{c_k}]((\sum_{i=0}^{k} x_i)^m \cdot h(\mathbf{x})) \neq 0$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1 \text{ (consequently m < p).}$$

Proof. Suppose indirectly that the inequality does not hold (and hence $m \geq p$), then we may define $E \subseteq Z_p$ such that E is a multi-set containing m elements and $\oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Let $Q(\mathbf{x}) = h(\mathbf{x}) \prod_{e \in E} \left(\sum_{i=0}^{k} x_i - e \right)$. By our construction we must have that $Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in \prod_{i=0}^{k} A_i$ as either $h(\mathbf{x}) = 0$ or $\sum_{i=0}^{k} x_i \in \oplus_h \sum_{i=0}^{k} A_i \subseteq E$. Furthermore $\deg(Q) = m + \deg(h) = \sum_{i=0}^{k} c_i$ by construction. From this we see $m \geq \sum_{i=0}^{k} c_i$ and hence $[x_0^{c_0} \ldots c_k^{c_k}]Q \neq 0$ (as it is binomial in nature).

Therefore, applying Combinatorial Nullstellenstaz (Theorem 1.2) yields an $\mathbf{a} \in A$ such at $Q(\mathbf{a}) \neq 0$ ↯. Thus $m < p$ and $\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq m + 1$. □

With this powerful result proven let us now take specific functions for h and prove superior lower bounds where possible. First, we examine the function $h(a_0, \ldots, a_k) = \prod_{0 \leq i < j \leq n} (a_i - a_j)$:

Theorem 3.3 (Restricted Sumset Theorem[1])**.** For a prime p, nonempty $A_0, A_1, \ldots, A_k \subseteq Z_p$ with $|A_i| \neq |A_j|$ for any $i \neq j$ and for the h defined above. If $\sum_{i=0}^{k} |A_i| \leq p + \binom{k+2}{2} - 1$, then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geq \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

A special case of this theorem for only two sets is the following:

Theorem 3.4 (Erdős-Heilbronn Conjecture[1])**.** For a prime p and nonempty $A, B \subseteq Z_p$, then $|A \oplus_h B| \geq \min\{p, |A| + |B| - \delta\}$ where $\delta = 3$ for the case $A = B$ and $\delta = 2$ in all other cases.

In order to prove these theorems, let us first state and prove a lemma concerning the coefficient of a particular polynomial:

Lemma 3.1. Let $0 \leq c_0, \ldots, c_k \in \mathbb{Z}$ and define $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$ (it is trivial that m is nonnegative). Then,

$$[x_0^{c_0} \ldots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right)^m \prod_{k \geq i > j \geq 0} (x_i - x_j) \right) = \frac{m!}{c_0! c_1! \ldots c_k!} \prod_{k \geq i > j \geq 0} (c_i - c_j).$$

Provide proof of this lemma based on proof of Ballot problem

With this out of the way, we now prove proposition 2.4:

Proof of Restricted Sumset Theorem . For this proof we will take the aforementioned

$$h(\mathbf{x}) = \prod_{0 \leq i < j \leq k} (x_i - x_j).$$

Now, let us define $c_i = |A_i| - 1$ and $m = \sum_{i=0}^{k} c_i - \binom{k+1}{2}$. Rearranging the assumptions of this theorem yields $\sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1 \leq p$ and, applying the trivial combinatorial identity $\binom{k+2}{2} = \binom{k+1}{2} + (k+1)$ yields

$\sum_{i=0}^{k} c_i - \binom{k+1}{2} + 1 = m + 1 \leq p$ (hence $m < p$). Then

$$[x_0^{c_0} \ldots x_k^{c_k}] \left(\left(\sum_{i=0}^{k} x_i \right) h \right) = \frac{m!}{c_0! \ldots c_k!} \prod_{0 \leq i < j \leq k} (c_i - c_j).$$

We know this product to be nonzero modulo p as $c_i \neq c_j$ for $i \neq j$ by construction and $m < p$. Finally, as the coefficient is nonzero and as $\deg(h) = \binom{k+2}{2}$ (as there are $k+2$

possible x_i's and each term of the product will contain two distinct x_i's so there are $\binom{k+2}{2}$ terms each of degree 1), we have $m = \sum_{i=0}^{k} c_i - \deg(h)$. Hence, applying theorem 2.3 yields $\left|\oplus_h \sum_{i=0}^{k} A_i\right| \geq m + 1 = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1$ by construction. □

We conclude this section with the proof of the Erdős-Heilbronn Conjecture:

Proof of Erdős-Heilbronn Conjecture. □

Ask grynkiewicz about this as Alons paper says $+\deg(h)$ instead of minus

Add proof

3.2 Graphs, Cubes, and Colorings

Now, we present a few combinatorial results of graph theory using the Combinatorial Nullstellensatz. For these proofs assume all graphs are loopless,

Theorem 3.1 ([1]). Let p be an odd prime and G ,a graph with $\frac{\sum_{i\in V(G)} d(i)}{e(G)} = d(G) > 2p-2$ and $\Delta \leq 2p-1$, we find a p-regular subgraph.

Proof. Let $B = (b_{i,e})_{i\in V(G), e\in E(G)}$ to be the incidence matrix of G, that being, $b_{i,j} = \begin{cases} 1, & i \in e \\ 0, & i \notin e \end{cases}$. For each $e \in E(G)$, let $x_e \in \{0,1\}$ be an associated variable and define

$$F : \{0,1\}^{e(G)} \longrightarrow \mathrm{GF}(p)$$

$$(x_e)_{e\in E(G)} \longmapsto F((x_e)_{e\in E(G)}) = \prod_{v\in V}\left[1 - \left(\sum_{e\in E} b_{v,e}x_e\right)^{p-1}\right] - \prod_{e\in E}(1-x_e).$$

Then, recall that $\frac{d(G)\cdot v(G)}{2} = e(G)$. Hence, we have $e(G) > \frac{2p-2}{2}v(G) = (p-1)v(G)$. And, as the highest order term of the first product has degree $(p-1)$ as each x_e within the sum has degree $p-1$ and the product over $v(G)$ terms of order $p-1$ is $v(G)(p-1)$, and the highest order term of the second product is $(-1)^{e(G)-1}\prod_{e\in E(G)} x_e$ of order $e(G)$, hence $\deg(F) = e(G)$. Then, as the highest order term is $\prod_{e\in E(G)} x_e^1$ with each $x_e \in \{0,1\}$, hence as $|\{0,1\}| - 1 = \deg(x_e)$, we see that applying combinatorial nullstellensatz yields an $(x_e)_{e\in E(G)=\mathbf{x}}$ such that $F(\mathbf{x}) \neq 0$ and as $F\left((0)_{e\in E(G)}\right) = 0$, we see $\mathbf{x} \neq (0)_{e\in E(G)}$. Hence, $\prod_{\mathbf{x}}(1-x_e) = 0$, so we see the first product is nonzero. Then, as $a^{p-1} \equiv 1 \pmod{p}$ for all $b \neq 0$, we see each $\sum_{e\in E(G)} b_{v,e}x_e = 0$, else the first product would be zero.

Now, let H be the subgraph induced by $E(H) = \{e \in E(G) : x_e = 1\}$ and note that as all terms of the sum $\sum_{e\in E} b_{v,e}x_e$ are either 0 or 1 and as there are precisely 2

$v \in V(G)$ such that $b_{v,e} = 1$ for each $e \in E(G)$, we see $p \mid |\{e \in E(G) : x_e = 1\}$, as p is an odd prime. Then, as $x_e = 1$ for all $e \in E(H)$, we see $\sum_{e \in E(H)} a_{v,e} x_e = \sum_{e \in E(H)} a_{v,e} = d_H(v)$ and as $p \mid e(H) = |\{e \in E(G) : x_e = 1\}|$, we see $p \mid d_H(v)$ for each $v \in V(H)$. Furthermore, as $d(v) < 2p$ for all $v \in H$, we see $d_H(v) = p$ for all $v \in V(H)$. Hence, H is p-regular.

□

Theorem 3.2 ([1])**.** Let p be a prime and let $G = (V, E)$ be a graph with $v(G) > d(p-1)$. Then, there is a nonempty $U \subseteq V(G)$ such that the number of cliques on d vertices of G intersecting U is a multiple of pb

Chapter 4

Zeilberger-Bressoud q-Dyson Theorem

The previous results have all been relatively simple applications of the Combinatorial Nullstellensatz. Now, we show its use in a more complex proof. We will construct a generalized laurent polynomial based on the subpower and prove the exact value of its constant term. To begin, recall the subpower,

Definition 4.1 (Subpower)**.** For a ring R, a $q \in \mathbb{R}$, and a $k \in \mathbb{N}_0$ we define

$$(x)_{k;q} = (1-x)\,(1-xq)\left(1-xq^2\right)\ldots\left(1-xq^{k-1}\right).$$

For convenience $(x)_{0;q} \coloneqq 1$.

As it is unnecessary in the following proofs, we will omit the q from notation so that $(x)_{k;q} = (x_k)$ for an assumed independent variable q.

For simplicity, when referring to this object we will call it the **subpower**, though this covention is not found in the literature and is simply adopted for convenience.

Now, let us state the Dyson conjecture originally conjectured in Dyson's paper [**?**] and proven by Wilson [8], with a much simpler proof similar to the one presented here provided by Good [3]. We will not prove it directly as its result will follow directly from the $q = 1$ case of the q-Dyson conjecture.

Theorem 4.1 (Dyson Conjecture)**.**

$$[x_1^0 \ldots x_n^0]\left(\prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}\right) = \frac{(\sum_{i=1}^n a_i)!}{\prod_{i=1}^n (a_i!)}.$$

A direct generalization of this, the Zeilberger-Bressoud q-Dyson conjecture was originally posed by Andrews in 1975 [2] and this proof was published by Károlyi and Nagy.

Theorem 4.2 (q-Dyson Conjecture [5])**.** First, let us define the following polynomial:

$$f_q(\mathbf{x}) = f_q(x_1, x_2, \ldots, x_n) \coloneqq \prod_{1 \le i < j \le n} \left(\frac{x_i}{x_j}\right)_{a_i} \left(\frac{q x_j}{x_i}\right)_{a_j}.$$

Then,

$$[x_1^0 \ldots x_n^0] f_q(\mathbf{x}) = \frac{(q)_{\sum_{i=1}^n a_i}}{\prod_{j=1}^n (q)_{a_j}}.$$

Before we can prove this result, we must examine a related function and prove a result about its coefficients. Note that this lemma is actually equivalent to the Combinatorial Nullstellenstatz.

Lemma 4.1. Let $\mathbb{F}$ be a field and $F \in \mathbb{F}[x_1, \ldots, x_n]$ to be a polynomial of degree $d \le \sum_{i=1}^n d_i$. For arbitrary $A_1, \ldots, A_n \subseteq F$ with $|A_i| = d_i + 1$ for each $1 \le i \le n$, we find

$$\left[\prod_{i=1}^n x_i^{d_i}\right] F = \sum_{c_1 \in A_1, c_2 \in A_2, \ldots, c_n \in A_n} \frac{F(c_1, c_2, \ldots, c_n)}{\varphi_1'(c_1)\varphi_2'(c_2)\ldots\varphi_n'(c_n)}$$

with $\varphi_i(z) = \prod_{a \in A_i}(z - a)$.

Proof. We construct a sequence of polynomials. Let $F_0 = F$ and define F_i as follows. Let $F_i(\mathbf{x}) = \frac{F_{i-1}}{\varphi_i(x_i)}$ in the ring $\mathbb{F}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. We see this construction guarantees $\left[\prod_{i=1}^n x_i^{d_i}\right] F_{i-1} = \left[\prod_{i=1}^n x_i^{d_i}\right] F_i$ and for all $\mathbf{c} \in \prod_{i=1}^n A_i$ we see $F_n(\mathbf{c}) = F(\mathbf{c})$ and $\deg_{x_i}(F_i) \le d_i$ for all $1 \le i \le n$, hence as $\sum_{i=1}^n |A_i| > \deg(F)$, we see lagrangian interpolation yields a unique polynomial of the form

$$F_n(\mathbf{x}) = \sum_{\mathbf{c} \in \prod_{i=1}^n A_i} F(\mathbf{c}) \prod_{i=1}^n \prod_{\gamma \in A_i \setminus c_i} \frac{x_i - \gamma}{c_i - \gamma}..$$

Then, we note for $\varphi_i(z) = \prod_{a \in A_i}(z - a)$, we find $\varphi_i'(z) = \sum_{a_k \in A_i} \prod_{i = a \in A_i \setminus a_k}(z - a)$, and evaluating at a $c_i \in A_i$ yields $\varphi'(c_i) = \prod_{a \in A_i \setminus c_i}(c_i - a)$. Then, we note that

$\left[\prod_{i=1}^{n} x_i^{d_i}\right] F_n(\mathbf{x}) = \sum_{c\in\prod_{i=1}^{n} A_i} \frac{F(\mathbf{c})}{\prod_{i=1}^{n}\prod_{\gamma\in A_i\setminus c_i}(c_i-\gamma)} = \frac{F(\mathbf{c})}{\prod_{i=1}^{n}\varphi_i'(c_i)}$. This completes the lemma. □

Proof of q-Dyson Conjecture. First, we note that if $a_i = 0$, then $(x)_{a_i} = (1-x)$, hence we may omit all of these terms as they will not affect the constant. Hence, we know each (relevant) a_i is a positive integer. Let

$$F(\mathbf{x}) = \prod_{1\le i<j\le n}\left(\prod_{i=0}^{a_i-1}\left(x_j - x_i q^t\right)\cdot\prod_{t=1}^{a_j}\left(x_i - x_j q^t\right)\right).$$

Denote $\kappa = \frac{1}{\prod_{1\le i<j\le n} x_i^{a_j} x_j^{a_i}}$. Then, we see

$$\begin{aligned}
f_q(x_1, x_2, \ldots, x_n) &= \prod_{1\le i<j\le n}[\prod_{k=1}^{a_i}\left(1-\frac{x_i}{x_j}q^{k-1}\right)\prod_{k=1}^{a_j}\left(1-\frac{x_j}{x_i}q^{k}\right)] \\
&= \prod_{1\le i<j\le n}\frac{1}{x_j^{a_i}x_i^{a_j}}[\prod_{k=1}^{a_i}\left(x_j - x_i q^{k-1}\right)\prod_{i=1}^{a_j}\left(x_i - x_j q^{k}\right)] \\
&= \frac{1}{\prod_{1\le i<j\le n} x_i^{a_j}x_j^{a_i}}\underbrace{\prod_{1\le i<j\le n}[\prod_{k=1}^{a_i}\left(x_j - x_i q^{k-1}\right)\prod_{k=1}^{a_j}\left(x_i - x_j q^{k}\right)]}_{=F(x_1,x_2,\ldots,x_n)} \\
&= \kappa\prod_{1\le i<j\le n}\left(x_j^{a_i}+\beta_i\right)\left(x_i^{a_j}+\beta_j\right) \\
&= \kappa\prod_{1\le i<j\le n}\left(x_j^{a_i}x_i^{a_j}+\beta_{ij}\right) \\
&= c\kappa(\prod_{1\le i<j\le n} x_j^{a_i}x_i^{a_j}) + \beta,
\end{aligned}$$

where $\beta_i, \beta_j, \beta_{ij}, \beta$ are all of the lower order terms from their respective product. We see the first term is simply a constant, and we see as the exponent of x_i will take on all values, a_k, except a_i and similarly, the exponent of x_j will take on all values except a_j. Hence, we find $[1]\, f_q(\mathbf{x}) = \left[\prod_{i=1}^{n} x_i^{\sum_{k=1}^{n} a_k - a_i}\right] F(\mathbf{x})$.

Now, we define $\sum_{i=1}^{n} a_i = \sigma$, $A_i = \{1, q, \ldots, q^{\sigma-a_i}\}$ and a sequence $\sigma_0 = 0$, $\sigma_i = \sum_{j=1}^{i-1} a_j$ for $2 \le i \le n+1$. It is clear $|A_i| = \sigma - a_i + 1$ and $\sigma_{n+1} = \sigma$. Now, we aim

to prove that for $\mathbf{c} = (c_1, \ldots, c_n) \in \prod_{i=1}^{n} A_i$, we have $F(\mathbf{c}) = 0$ unless $c_i = q^{\sigma_i}$ for each $1 \leq i \leq n$.

We will suppose a contradiction, that is there exists a $(c_1, c_2, \ldots, c_n) = \mathbf{c} \in \prod_{i=1}^{n} A_i$ such that $F(\mathbf{c}) \neq 0$ for $c_i = q^{\alpha_i}$ where $0 \leq \alpha_i \leq \sigma - a_i$. Then, we see for a pair $j > i$, we have $\alpha_j - \alpha_i \geq a_i$, in particular every pair α_j, α_i with $i \neq j$ is distinct. Then, we see their is a unique ordering π such that $\alpha_{\pi(1)} < \alpha_{\pi(2)} < \ldots < \alpha_{\pi(n)}$. Then, summing over the inequality $\alpha_{\pi(i+1)} - \alpha_{\pi(i)} \geq a_{\pi(i)}$ for $1 \leq i \leq n-1$ yields

$$\begin{aligned}\left(\alpha_{\pi(_n)} - \alpha_{\pi(n-1)}\right) + \left(\alpha_{\pi(n-1)} - \alpha_{\pi(n-2)}\right) + \ldots + \left(\alpha_{\pi(2)} - \alpha_{\pi(1)}\right) &= \alpha_{\pi(n)} - \alpha_{\pi(1)} \\ &\geq \sum_{i=1}^{n-1} a_{\pi(i)} \\ &= \sigma - a_{\pi(n)}.\end{aligned}$$

Then, as $\alpha_{\pi(1)} \geq 0$ and $\alpha_{\pi(n)} \leq \sigma - a_{\pi(n)}$ by the original inequality, we find equality must hold, hence

$$\alpha_{\pi(n)} - \alpha_{\pi(1)} = \sigma - a_{\pi(n)} = \sigma_n.$$

We see this summation works over $k < n-1$ terms as well, so $\alpha_{\pi(k)} = \sigma_k$ hence π must be the identity permutation and we see $\alpha_k = \sum_{i=1}^{k-1} a_i = \sigma_k$ for all $1 \leq k \leq n$. $\lightning$. Hence, we see $F(\mathbf{c}) = 0$ unless each $c_i = q^{\sigma_i}$, so the constant

$$[1]\, f_q = \frac{F\left(q^{\sigma_1}, \ldots, q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right) \ldots \varphi_n'\left(q^{\sigma_n}\right)}$$

by the lemma.

Now, denote $\tau_i = \binom{\sigma_i}{2} + \sigma_i\left(\sigma - \sigma_i + 1\right)$ and we derive a subpower form of $\varphi_i'\left(q^{\sigma_i}\right)$.

Then we see

$$\begin{aligned}
\varphi_i'\left(q^{\sigma_i}\right) &= \prod_{\substack{0\le t\le \sigma-a_i \\ t\neq\sigma_i}} \left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}\left(q^{\sigma_i}-q^t\right)\prod_{t=\sigma_i+1}^{\sigma-a_i}\left(q^{\sigma_i}-q^t\right) \\
&= \prod_{t=0}^{\sigma_i-1}(-q)^t\left(1-q^{\sigma_i-t}\right)\prod_{t=1}^{\sigma-\sigma_i-a_i} q^{\sigma_i}\left(1-q^t\right) \\
&= (-1)^{\sigma_i}\cdot \underbrace{\prod_{i=1}^{\sigma_i-1} q^t}_{=q^{\sum_{i=1}^{\sigma_i-1}1}=q^{\frac{\sigma_i(\sigma_i-1)}{2}}=q^{\binom{\sigma_i}{2}}} \cdot \underbrace{\prod_{i=0}^{\sigma_i-1}(1-q^{\sigma_i-t})}_{=(q)_{\sigma_i}} \cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}} q^{\sigma_i}}_{=q^{\sigma_i(\sigma-\sigma_{i+1})}} \cdot \underbrace{\prod_{i=1}^{\sigma-\sigma_{i+1}}\left(1-q^t\right)}_{=(q)_{\sigma-\sigma_{i+1}}} \\
&= (-1)^{\sigma_i} q^{\binom{\sigma_i}{2}+\sigma_i(\sigma-\sigma_{i+1})}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}} \\
&= (-1)^{\sigma_i} q^{\tau_i}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}.
\end{aligned}$$

Similarly by double counting the terms and performing simple manipulations, we find $F\left(q^{\sigma_1},\ldots,q^{\sigma_n}\right)$ in a subpower form. First, note that we can write a partial sequence from $(\sigma_j-\sigma_i-a_i)=(\sigma_j-\sigma_{i+1})$ to $(\sigma_j-\sigma_i)$ as

$$\prod_{t=0}^{a_i-1}\left(1-q^{\sigma_j-\sigma_i-t}\right)=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i-a_i}(1-q^t)}=\frac{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_{i+1}}(1-q^t)}=\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}.$$

Similarly, we find a partial sequence from $(\sigma_j-\sigma_i)$ to $(\sigma_j+a_j-\sigma_i)=(\sigma_{j+1}-\sigma_i)$ to be

$$\prod_{t=1}^{a_j}\left(1-q^{\sigma_j-\sigma_i+t}\right)=\frac{\prod_{t=1}^{\sigma_j+a_j-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}=\frac{\prod_{t=1}^{\sigma_{j+1}-\sigma_i}(1-q^t)}{\prod_{t=1}^{\sigma_j-\sigma_i}(1-q^t)}=\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}}.$$

Now, let $u=\sum_{i=1}^{n}(n-i)\,a_i$ and $v=\sum_{i=1}^{n}\left[(n-i)\left(a_i+\sigma_i+\binom{a_i}{2}\right)+\sigma_i(\sigma-\sigma_{i+1})\right]$

and we see

$$
\begin{aligned}
F\left(q^{\sigma_1}, q^{\sigma_2}, \ldots, q^{\sigma_n}\right) &= \prod_{1\le i<j\le n}\left(\prod_{t=0}^{a_i-1}\left(q^{\sigma_j}-q^{\sigma_i}q^t\right)\cdot\prod_{t=1}^{a_j}\left(q^{\sigma_i}-q^{\sigma_j}q^t\right)\right)\\
&= \prod_{1\le i<j\le n}(-1)^{a_i}\left(\underbrace{\prod_{t=0}^{a_i-1}q^{\sigma_i+t}}_{=q^{a_i\sigma_i}q^{\binom{a_i}{2}}}\underbrace{\prod_{t=0}^{a_i-1}(1-q^{\sigma_j-\sigma_i-t})}_{=\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}}\cdot\underbrace{\prod_{t=1}^{a_j}q^{\sigma_i}}_{=q^{\sigma_i(\sigma-\sigma_{i+1})}}\underbrace{\prod_{t=1}^{a_j}\left(1-q^{\sigma_j-\sigma_i+t}\right)}_{=\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}}}\right)\\
&= (-1)^{\sum_{i=1}^n(n-i)a_i}\,q^{\sum_{i=1}^n\left[(n-i)(a_i\sigma_i+\binom{a_i}{2})+\sigma_i(\sigma-\sigma_{i+1})\right]}\prod_{1\le i<j\le n}\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}\\
&= (-1)^u\,q^v\frac{\prod_{i=1}^{n-1}\prod_{j=i+1}^{n}(q)_{\sigma_{j+1}-\sigma_i}}{\prod_{i=1}^{n-1}\prod_{j=i+1}^{n}(q)_{\sigma_j-\sigma_{i+1}}}\\
&= (-1)^u\,q^v\frac{\prod_{i=1}^{n-1}\prod_{j=i+2}^{n+1}(q)_{\sigma_j-\sigma_i}}{\prod_{i=2}^{n}\prod_{j=i}^{n}(q)_{\sigma_j-\sigma_i}}\\
&= (-1)^u\,q^v\frac{\prod_{j=3}^{n+1}(q)_{\sigma_j-\sigma_1}(\prod_{i=2}^{n-1}\prod_{j=i+2}^{n}(q)_{\sigma_j-\sigma_i})(\prod_{i=2}^{n-1}(q)_{\sigma_{n+1}-\sigma_i})}{(\prod_{i=2}^{n-1}\prod_{j=i+2}^{n}(q)_{\sigma_j-\sigma_i})(\prod_{i=2}^{n-1}\prod_{j=i}^{i+1}(q)_{\sigma_j-\sigma_i})}\\
&= (-1)^u\,q^v\frac{\prod_{i=2}^{n-1}(q)_{\sigma-\sigma_i}\prod_{j=3}^{n+1}(q)_{\sigma_j-\sigma_1}}{\prod_{i=2}^{n-1}(q)_{\sigma_{i+1}-\sigma_i}}\cdot\frac{(q)_{\sigma_2-\sigma_1}}{(q)_{\sigma_2-\sigma_1}}\cdot\frac{(q)_{\sigma-\sigma_n}}{(q)_{\sigma-\sigma_n}}\underbrace{(q)_{\sigma_1-\sigma_1}}_{1}\\
&= (-1)^u\,q^v\frac{\prod_{i=2}^{n}(q)_{\sigma-\sigma_i}\cdot(q)_{\sigma-\sigma_1}\cdot\prod_{i=1}^{n}(q)_{\sigma_i}}{\prod_{i=1}^{n}(q)_{\sigma_{i+1}-\sigma_i}}\\
&= (-1)^u\,q^v\prod_{i=1}^{n}\frac{(q)_{\sigma_i}(q)_{\sigma-\sigma_i}}{(q)_{\sigma_{i+1}-\sigma_i}}.
\end{aligned}
$$

From here, we see

$$\begin{aligned}\sum_{i=1}^{n}(n-i)\,a_i &= (n-1)\,a_1+(n-2)\,a_2+\ldots+0a_n\\ &= \sum_{i=1}^{n-1}a_i+\sum_{i=1}^{n-2}a_i+\ldots+\sum_{i=1}^{1}a_i+\underbrace{\sum_{i=1}^{0}a_i}_{0}\\ &= \sigma_n+\sigma_{n-1}+\ldots+\sigma_2+\underbrace{\sigma_1}_{0}\\ &= \sum_{i=1}^{n}\sigma_i.\end{aligned}$$

Hence, $u=\sum_{i=1}^{n}\sigma_i$ and the powers of -1 will vanish. Moreover, we show by induction that the powers of q vanish, that is $\sum_{i=1}^{n}(n-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{n}\binom{\sigma_i}{2}$. Note that for $j=0$, we have $\sum_{i=1}^{0}(0-i)\left(a_i\sigma_i+\binom{a_i}{2}\right)=\sum_{i=1}^{0}\binom{\sigma_i}{2}=0$. Similarly, the case $n=1$ holds. Then, for the general case, we simply expand the right hand side as follows:

$$\sum_{i=2}^{n}\binom{\sigma_i}{2}=\binom{\sigma_2}{2}+\ldots+\binom{\sigma_n}{2} \tag{4.1}$$

$$=\frac{1}{2}\Big[(a_1-1)\,a_1+(a_1+a_2-1)\,(a_1+a_2)+\ldots+(a_1+\ldots+a_{n-1}-1)\,(a_1+\ldots+a_{n-1})\Big] \tag{4.2}$$

Let us examine the First, grouping the squares and the terms involving -1 and then

grouping the remaining products yields

$$
\begin{aligned}
&(a_1 + \ldots + a_{n-1} - 1)(a_1 + \ldots + a_{n-1}) \\
&\qquad = a_{n-1}^2 - a_{n-1} + a_{n-2}^2 - a_{n-2} + \ldots + a_1^2 - a_1 + \\
&\qquad + a_{n-1}(a_1 + \ldots + a_{n-2}) + a_{n-2}(a_1 + \ldots + a_{n-3}) + a_{n-2}a_{n-1} \\
&\qquad + a_{n-3}(a_1 + \ldots + a_{n-4}) + a_{n-3}(a_{n-2} + a_{n-1}) + \ldots \\
&\qquad + a_3(a_1 + a_2) + a_3(a_4 + \ldots + a_{n-1}) + a_2a_1 + a_2(a_3 + \ldots + a_{n-1}) \\
&\qquad + a_1(a_2 + \ldots + a_{n-1}).
\end{aligned}
$$

Collecting terms yields

$$
= (a_{n-1} - 1)a_{n-1} + \ldots + (a_1 - 1)a_1 + 2a_{n-1}\sigma_{n-1} + \ldots + 2a_2\sigma_2.
$$

Applying this identity to 4.2 and adding zero terms where necessary gives the result:

$$
\begin{aligned}
\sum_{i=2}^{n} \binom{\sigma_i}{2} &= a_{n-1}\sigma_{n-1} + \binom{a_{n-1}}{2} + 2\left(a_{n-2}\sigma_{n-2} + \binom{a_{n-2}}{2}\right) + \ldots + (n-2)\left(a_2\sigma_2 + \binom{a_2}{2}\right) \\
&= \sum_{i=1}^{n-i} (n-i)\left(a_i\sigma_i + \binom{a_i}{2}\right).
\end{aligned}
$$

Assembling all results yields

$$
\begin{aligned}
[1]\, f_q(\mathbf{x}) = \frac{F\left(q^{\sigma_1}, \ldots, q^{\sigma_n}\right)}{\varphi_1'\left(q^{\sigma_1}\right) \ldots \varphi_n'\left(q^{\sigma_n}\right)} &= \prod_{i=1}^{n} \frac{(q)_{\sigma_i}(q)_{\sigma-\sigma_i}}{(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}}(q)_{\sigma_{i+1}-\sigma_i}} \\
&= \frac{(q)_{\sigma-\sigma_1}}{\prod_{i=1}^{n}(q)_{\sigma_{i+1}-\sigma_i}} \\
&= \frac{(q)_{\sigma}}{\prod_{i=1}^{n}(q)_{a_i}} \\
&= \frac{(q)_{a_1+a_2+\ldots+a_n}}{(q)_{a_1}\ldots(q)_{a_n}}.
\end{aligned}
$$

□

Chapter 5

Chevalley-Warning Theorem and Reiher's Proof of the Kemnitz Conjecture

5.1 Chevalley-Warning Theorem

Our first major result of this section concerns the theorem of Chevalley and Warning which declares the conditions under which a certain nontrivial solution to a polynomial in a finite field of characteristic p can exist:

Theorem 5.1 (Chevalley-Warning Theorem)**.** Let F be a finite field of characteristic p and let $f_1, f_2, \ldots, f_k \in F[x_1, x_2, \ldots, x_n]$ be polynomials and N to be the number of points $\mathbf{x} \in F^n$ such that $f_1(\mathbf{x}) = \ldots = f_k(\mathbf{x}) = 0$. If $\sum_{i=1}^{k} \deg(f_i) < n$, then $N \equiv 0 (\text{mod } p)$.

In order to provide a proof of this statement, let us first state and prove the following lemma:

Lemma 5.1 (Lemma)**.** Let F be a finite field and $k_1, k_2, \ldots, k_n \geq 0$ such that $\min_{1 \leq i \leq n} k_i \leq |F| - 2$. Then, $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = 0$. (Note: if a 0^0 occurs in the expressions it will be treated as a 1).

Proof. Assume without loss of generality that $k_1 < |F| - 1$. Then, by factoring out a $x_1^{k_1}$ from each term of the sum and grouping all such x_1's, we have $\sum_{x_1, x_2, \ldots, x_n \in F} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n} = \left(\sum_{x_1 \in F} x_1^{k_1}\right) \sum_{x_2, \ldots, x_n \in F} x_2^{k_2} \ldots x_n^{k_n}$, hence we must only show that $\sum_{x_1 \in F} x_1^{k_1} = 0$. Suppose $k_1 = 0$, then $\sum_{x_1 \in F} x_1^{k_1} = |F|$ and, since p divides $|F|$ we see the case $k_1 = 0$ is trivially true. Now, let $\omega \in F^{\times}$ be a generator of $F^{\times}$. Then, we have that

$$\sum_{x_1 \in F} x_1^{k_1} = \sum_{x_1 \in F^{\times}} x_1^{k_1} = \sum_{x_1 \in F^{\times}} (\omega x)^{k_1} = \omega^{k_1} \sum_{x_1 \in F^{\times}} x_1^{k_1} = \omega^{k_1} \sum_{x_1 \in F} x_1^{k_1}.$$

Taking the difference of the first and last terms of the above equality yields

$\left(\omega^{k_1}-1\right)\left(\sum_{x_1\in F} x_1^{k_1}\right)=0$, so we must have either the sum is 0 or $\omega^{k_1}-1=0$. However, as ω is a generator of the cyclic group $F^{\times}$, we may only have that $\omega^{k_1}=1$ if $k_1\equiv -1 \pmod{|F|}$. But, as $0<k_1<|F|-1$ this case cannot occur, hence we see $\sum_{x_1\in F} x_1^{k_1}=0$, so the lemma is proven. □

Proof of Chevalley-Warning Theorem. Recalling that $x^{|F|}=x$ (and thus $x^{|F|-1}=1$ for nonzero x). Then, define

$$M=\sum_{\mathbf{x}\in F^n}\prod_{i=1}^{k}\left(1-f_i\left(\mathbf{x}\right)^{|F|-1}\right).$$

We see, by the earlier proposition, that a term of the sum will be 1 if and only if **x** is a solution to the system $f_1, f_2, \ldots, f_k$, else it will be 0. Furthermore, it is clear by the construction that M will be exactly equal to the number of solutions to our system $f_1, \ldots, f_k$, and hence it precisely N.

Now, let us define the product from our construction to be a polynomial g, that is $g\left(\mathbf{x}\right)=\prod_{i=1}^{k}\left(1-f_i\left(\mathbf{x}\right)^{|F|-1}\right)$. Then, repeatedly applying the substitution $x_j^{|F|}\to x_j$ to g yields a polynomial $\overline{g}=g$ for all $\mathbf{x}\in F^n$. Furthermore, $\deg_{x_j}\left(\overline{g}\right)\leq |F|-1$ for $1\leq j\leq n$(This is clear as , if it were not we would be able to apply the substitution once again). Then, substituting $\overline{g}$ in place of g yields

$$M=\sum_{\mathbf{x}\in F^n}\overline{g}\left(\mathbf{x}\right).$$

Then, applying our lemma, we see that all monomials with degree $|F|-2$ or less will equal 0 and hence the only possible nonzero terms of $\overline{g}$ are those of the form $\prod_{i=1}^{n} x_i^{|F|-1}$. Expanding the product, we see that such a monomial would be of degree $n\left(|F|-1\right)$, however as $\deg f_i^{|F|-1}=\left(|F|-1\right)\deg\left(f_i\right)$, we see that $\deg\left(g\right)\leq\left(|F|-1\right)\sum_{i=1}^{k} f_i<n\left(|F|-1\right)$ by construction. Consequently, any such

monomial of $\overline{g}$ (and hence g) will have a zero coefficient, and thus

$M = N \equiv 0 \pmod{p}$. □

5.2 Proof of Kemnitz Conjecture

This theorem has found many uses in combinatorics and number theory. One of its most potent results is Reiher's proof of the Kemnitz conjecture. This proof makes heavy use of the Chevalley-Warning Thoerem, as we will see. Before, we can state the theorem, however, we must define a few concepts.

Definition 5.1. We define $f(n,k)$ to be the minimal number f such that any set of f k-tuples of integers will contain a subset of cardinality n, whose sum is congruent to $0 \mod n$.

Given a set of tuples X, we define the symbol $(n \mid X)$ to be the number of subsets $Y \subseteq X$ so that $|Y| = n$ and $\sum_{y \in Y} y \equiv 0 \mod n$.

One notable result involving the first function is that of Erdos, Ginzburg, and Ziv that $f(n,1) = 2n-1$. That is, given any sequence of integers of size greater or equal to $2n-1$, we always find a subsequence whose sum is congruent to n. As it turns out other such constants are much more difficult to compute. The following was conjectured by Kemnitz:

Theorem 5.1 (Kemnitz Conjecture)**.**

$$f(n,2) = 4n-3$$

.

As it turns out, it suffices to show that $f(p,2) \leq 4p-3$ for a given prime p. Taking the points $(1,1), (-1,1)(1,-1), (-1,-1)$ each $n-1$ times for a total of $4n-4$ yields a set not containing any sequences congruent to 0, hence this proves the lower bound.

Moreover, one finds that the set of primes p, satisfying equality to be closed under multiplication, hence one need only show the fact to hold true for primes.

Before we can prove the main statement, we need to prove several smaller lemmas, though many of the proofs will be quite analogous to each other.

Lemma 5.1. Given a set J of ordered pairs with $|J| = 3p - 3$ we find

$$1 - (p-1 \mid J) - (p \mid J) + (2p-1 \mid J) + (2p \mid J) \equiv 0.$$

Proof. To prove this lemma one makes use of Chevalley and Warning's theorem in the field $\mathbf{F}_p$. First, denote the elements of J to be (a_i, b_i) for $1 \leq i \leq 3p-3$. Then, define the following three polynomials $f_1, f_2, f_3 \in F[x_1, \ldots, x_{3p-2}]$ by

$$\begin{aligned} f_1 &= \sum_{i=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1} \\ f_2 &= \sum_{i=1}^{\infty} a_n x_n^{p-1} \\ f_3 &= \sum_{i=1}^{3p-3} b_n x_n^{p-1}. \end{aligned}$$

Then, we note that $x_n^{p-1} = 1$ for all $x_n \neq 0$ (of which there are $p-1$). Moreover, assuming $x_{3p-2} = 0$, we find $\sum_{i=1}^{3p-3} x_n^{p-1} = 0$ only in the following cases

1. $x_i = 0$ for all $1 \leq i \leq 3p-3$,
2. $x_i \neq 0$ for precisely p integers $1 \leq i \leq 3p-3$,
3. $x_i \neq 0$ for precisely $2p$ integers $1 \leq i \leq 3p-3$.

Assuming the first case, we find 1 trivial zero. Moreover, this will clearly be a solution to f_2 and f_3 as well.

For the second case we find there are $p-1$ possibilities for each x_i which is nonzero yielding $(p-1)^p$ permutations for a given solution. We see a given combination

will satisfy $f_2 = f_3 = 0$ only if the subsequence (a_{n_k}, b_{n_k}) induced by taking only the nonzero elements is a sequence of zero sum. In this case we see there are precisely $(p \mid J)$ possible subsequences. Putting this together yields $(p-1)^p (p \mid J)$ solutions for case 2.

Case 3 follows similar reasoning. We find $(p-1)^{2p}$ permutations of any given solution to f_2, f_3. And the number of solutions to $f_2 = f_3 = 0$ is precisely the number of zero sum subsequences of length $2p$, $(2p \mid J)$, up to permutations if the x_i's. Accounting for permutations yields $(p-1)^{2p} (2p \mid J)$ solutions in case 2.

Next, assuming $x_{3p-2} \neq 0$ we see there are now two possibilities for a solution to f_1,

1. $x_i \neq 0$ for precisely $p-1$ integers $0 \leq i \leq 3p-3$, or
2. $x_i \neq 0$ for precisely $2p-1$ integers $0 \leq i \leq 3p-3$.

In both cases, the same argument produces the result yielding a cumulative $(p-1)^p (p-1 \mid J) + (p-1)^{2p} (2p-1 \mid J)$ solutions when $x_{3p-2} \neq 0$. Totaling, we find

$$1 + (p-1)^p (p \mid J) + (p-1)^{2p} (2p \mid J) + (p-1)^p (p-1 \mid J) + (p-1)^{2p} (2p-1 \mid J)$$

solutions to $f_1 = f_2 = f_3 = 0$. Since $(p-1)^p \equiv (-1)^p \equiv -1$ and $(p-1)^{2p} \equiv ((-1)^p)^2 \equiv 1$, we find the result follows by simply applying the Chevalley-Warning theorem. □

The following lemma all follow from essentially the same argument using the given set of polynomials:

Lemma 5.2.

If $|J| = 3p - 2$ or $|J| = 3p - 1$, then

$$1 - (p \mid J) + (2p \mid J) \equiv 0. \tag{5.1}$$

Moreover, $(p \mid J) \equiv 0$ implies $(2p \mid J) \equiv -1$.

Proof. The second assertion follows directly from the first, so we need only show claim 1. Again, we define the following polynomials

$$f_1 = \sum_{i=1}^{3p-m} x_n^{p-1}$$
$$f_2 = \sum_{i=1}^{3p-m} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{3p-m} b_n x_n^{p-1}.$$

Applying the same methods as the first lemma yields

$$1 + (p-1)^p (p \mid J) + (p-1)^{2p} (2p \mid J)$$

solutions. Evaluating the coefficients and applying Chevalley-Warning yields the result. □

Lemma 5.3. If $|J| = 4p - 3$, then

$$-1 + (p \mid J) - (2p \mid J) + (3p \mid J) \equiv 0 \text{ and,} \tag{5.2}$$
$$(p-1 \mid J) - (2p-1 \mid J) + (3p-1 \mid J) \equiv 0 \tag{5.3}$$

Proof. This is proved analogously to the previous lemmas. First, we show 5.2 by taking

the following polynomials

$$f_1 = \sum_{i=1}^{4p-3} x_n^{p-1}$$
$$f_2 = \sum_{i=1}^{4p-3} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{4p-3} b_n x_n^{p-1}.$$

Applying the same argument as the previous lemmas yields

$$1 + (p-1)^p (p \mid J) + (p-1)^{2p} (2p \mid J) + (p-1)^p (3p \mid J)$$

solutions. Evaluating the coefficients and applying Chevalley-Warning yields

$$1 - (p \mid J) + (2p \mid J) - (3p \mid J) \equiv 0.$$

Finally, negating this yields result 5.2.

Similarly, for 5.3 we use the polynomials

$$f_1 = \sum_{i=1}^{4p-3} x_n^{p-1} + x_{4p-2}^{p-1}$$
$$f_2 = \sum_{i=1}^{4p-3} a_n x_n^{p-1}$$
$$f_3 = \sum_{i=1}^{4p-3} b_n x_n^{p-1}.$$

Counting solutions yields

$$1 + (p-1)^p (p \mid J) + (p-1)^{2p} (2p \mid J) + (p-1)^{3p} (3p \mid J)$$
$$+ (p-1)^p (p-1 \mid X) + (p-1)^{2p} (2p-1 \mid X) + (p-1)^{3p} (3p-1 \mid X)$$

solutions. Evaluating coefficients and applying Chevalley-Warning theorem yields

$$1 - (p \mid J) + (2p \mid J) - (3p \mid J) - (p-1 \mid J) + (2p-1 \mid J) - (3p-1 \mid J) \equiv 0.$$

As we already know the first 4 terms to be congruent to 0 negating what is left yields the result. □

These lemmas make full use of the Chevalley-Warning theorem and show its power in proving these sorts of combinatorial results. Before we can present the proof of the main theorem (the Kemnitz conjecture) we need to prove a few more lemmas.

Lemma 5.4. If $|J| = 4p - 3$, then

$$3 - 2\,(p-1 \mid J) - 2\,(p \mid J) + (2p-1 \mid J) + (2p \mid J) \equiv 0. \tag{5.4}$$

Proof. Denoting $\mathscr{I}$ to be the set of all subsets $I \subseteq J$ with $|I| = 3p - 3$, we see

$$\sum_{I \in \mathscr{I}} [1 - (p-1 \mid I) - (p \mid I) + (2p-1 \mid I) + (2p \mid I)] \equiv 0. \tag{5.5}$$

We find there are $\binom{4p-3}{3p-3}$ possible sets I. Then, for a given zero sum subsequence of length $p-1$ in X, we see we can for a set $I \subseteq \mathscr{I}$ by simply appending $2p-2$ elements to the subsequence. We find there are $\binom{3p-2}{2p-2}$ possibilities for these appendices to form I. Similarly, given a zero sum subsequence of length p we find $\binom{3p-3}{2p-3}$ possible sets I containing the sequence. For a sequence of length $2p-1$ we find $\binom{2p-2}{p-2}$ possibilities and for a sequence of length $2p$, we find $\binom{2p-3}{p-3}$ possibilities.

Permuting over all such zero-sum sequences in J yields

$$(5.5) = \binom{4p-3}{3p-3} - \binom{3p-2}{2p-2}(p-1 \mid J) - \binom{3p-3}{2p-3}(p \mid J) + \binom{2p-2}{p-2}(2p-1 \mid J) + \binom{2p-3}{p-3}(2p \mid J) \equiv 0.$$

Expanding and reducing the binomial coefficients modulo p yields equation **??**. □

Before we may prove the main result we need just a few more lemmas:

Lemma 5.5. If a set of exactly ordered pairs J has a subset K with $|K| = 3p$ and $\sum_{k\in K} k \equiv 0$, then $(p \mid J) > 0$.

Proof. Let $q \in J$ be an abritrary element. We assume indirectly $(p \mid J) = 0$. Since J has no zero-sum subsequences of length p, we find $J - q$ still will not have such a subsequence (where $J - q$ denotes the set J excluding the element q), so $(p \mid J - q) = 0$. Applying the second conclusion of 5.2 yields $(2p \mid J - q) > 0$. Letting $k_i \in K$ be distinct elements of K, $1 \le i \le 3p$ we see $\sum_{i=1}^{3p} k_i = \sum_{i=1}^{p} k_i + \sum_{i=p+1}^{3p} k_i \equiv 0$ and $\sum_{i=p+1}^{3p} k_i > 0$ by the previous inequality, we find $\sum_{i=1}^{p} k_i > 0$, hence $(p \mid J) > 0$. □

We prove one final lemma:

Lemma 5.6. If $|X| = 4p - 3$ and $(p \mid X) = 0$, then

$$(p-1 \mid X) = (3p-1 \mid X). \tag{5.6}$$

Proof. Let N denote the number of partitions of X into 3 sets, A, B, C with

$$|A| = p-1, |B| = p-2, \text{ and } |C| = 2p \tag{5.7}$$

so that

$$\sum_{a\in A} a = \sum_{c\in C} c \equiv (0,0) \text{ and consequently } \sum_{b\in B} b \equiv \sum_{x\in X} x. \tag{5.8}$$

First, we note that

$$N \equiv \sum_{A} (2p \mid X - A)$$

where $\sum_A$ denotes the sum over all sets $A \subseteq X$ so that 5.7 and 5.8 hold. Note that this simply counts the number of admissible C for each possible set A, leaving whatever points remain to belong to B, thereby counting the number of possible partitions (modulo p). Next, since $|X - A| = 3p - 2$, we may apply 5.2 to see $N \equiv \sum_A -1$. Finally, we see this is simply the negation of the number of all subsets of X of size $p - 1$ with zero-sum, so by definition, $N \equiv -(p - 1 \mid X)$,

Applying the same method, but over B, we see $N \equiv \sum_B (2p \mid X - B)$, by counting all possible sets C for each admissible B. As $|X - B| = 3p - 1$, we may once again apply 5.2 to find $N \equiv \sum_{X-B} -1 \equiv -(3p - 1 \mid X)$, applying definitions to produce the final congruence.

By method of double counting we attain $(p - 1 \mid X) \equiv (3p - 1 \mid X)$, the desired result. □

With many small parts proven, we need simply combine them to produce the desired result, that $(p \mid X) \neq 0$ if $|X| = 4p - 3$.

Proof of Kemnitz Conjecture. Adding the equations we have obtained thus far, we see

$$(5.2) + (5.3) + (5.5) + (5.6) \text{ yields } 2 - (p \mid X) + (3p \mid X) \equiv 0. \tag{5.9}$$

Recalling that p was an odd prime, we see the statement $(p \mid X) \equiv (3p \mid X) \equiv 0$ cannot be true (as $2 \not\equiv 0$), Hence, either $(p \mid X) \not\equiv 0$ in which case the claim is shown, or $(3p \mid X) \not\equiv 0$ implying X contains a subset of size $3p$ whose sum is zero. Applying

lemma 5.5 then yields that $(p \mid X) > 0$, so the claim is shown in this case as well. Finally, using the already known statements about multiplicative closure and the special case $p = 2$ yields the full Kemnitz conjecture. $\square$

Chapter 6

Davenport constant of finite abelian p-groups

This theorem aims to prove one simple result, that being the davenport constant of an arbitrary finite abelian p-group.

Theorem 6.1. Let p be prime, $G = C_{q_1} \oplus C_{q_2} \oplus \ldots \oplus C_{q_d}$ with $q_i = p_i^{m_i}$ for some primes p_i and integers $m_i > 0$. Suppose $g_1, \ldots, g_m \in G$ is a sequence of (not necessarily distinct) terms from G. Then, if $m \geq 1 + \sum_{i=1}^{d} (q - 1)$, then there is a non-empty subset $I \subseteq [0, m]$ so that $\{g_i : i \in I\}$ is zero-sum.

The proof of this theorem will consist of many parts which, here, are broken into smaller lemmas and propositions for simplicity.

6.1 Map Functor

For the remainder of this proof, F will be a field, $m \geq 1$ will be an integer and $\{0, 1\}^m$ will denote the set of sequences consisting of all 0's and 1's taken from the vector space F^m.

Proposition 6.1. $\mathrm{Map}\left(\{0, 1\}^m, F\right)$ is an F-vector space with pointwise addition and composition multiplication. That is, for $f, g \in \mathrm{Map}\left(\{0, 1\}^m, F\right)$ we define $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(g(x))$.

Proof. This statement is routinely checked. First we show the map space to be an abelian group, then we verify composition produces a F-module and subsequently an F-vector

space. Associativity of the map space follows from associativity of F:

$$\begin{aligned}(f+(g+h))(x) &= f(x)+(g+h)(x)\\ &= f(x)+g(x)+h(x)\\ &= (f+g)(x)+h(x)\\ &= ((f+g)(h))(x).\end{aligned}$$

We choose the identity to be the zero map, denoted $\mathbf{0}$.

Additive inverses are satisfied by negation. For $f \in \mathrm{Map}(\{0,1\}^m, F)$, $f^{-1} = -f(x)$ which we find to be well-defined and within the map space, and $f + f^{-1} = f + (-f) = \mathbf{0}$.

Finally, commutativity is also inherited from F:

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x).$$

Now, we verify $\mathrm{Map}(\{0,1\}^m, F)$ is an F-module. Let $r, s \in F$ and $1 \in F$ to be the multiplicative identity of F.

We find, for some $\mathbf{x} \in \{0,1\}^m$, $(1f)(\mathbf{x}) = 1f(\mathbf{x}) = f(\mathbf{x})$.

Furthermore, associativity of composition holds :

$$((rs)f)(\mathbf{x}) = (rs)f(\mathbf{x}) = f((sf)(\mathbf{x})) = (r(sf))(\mathbf{x}).$$

Lastly, distributivity of composition also holds:

$$\begin{aligned}
((r+s)f)(\mathbf{x}) &= (r+s)f(\mathbf{x}) = rf(\mathbf{x}) + sf(\mathbf{x}) \\
&= (rf)(\mathbf{x}) + (sf)(\mathbf{x}) \\
&= (rf + sf)(\mathbf{x}) \\
\text{and } (r(f+g))(\mathbf{x}) &= r((f+g)(\mathbf{x})) \\
&= r(f(\mathbf{x}) + g(\mathbf{x})) \\
&= rf(\mathbf{x}) + rg(\mathbf{x}) \\
&= (rf)(\mathbf{x}) + (rg)(\mathbf{x}) \\
&= (rf + rg)(\mathbf{x})
\end{aligned}$$

.

As these properties hold for composition (multiplication) and the addition operation forms an abelian group, we have thus verifies $\mathrm{Map}(\{0,1\}^m, F)$ is an F-module. Since F is a field, it is then a F-vector space. □

Proposition 6.2. The function $h(\mathbf{x}) = \prod_{i=1}^{n}(1 - x_i)$ is the characteristic function of the vector $\mathbf{0} \in \{0,1\}^n$. Moreover, the set of all monomials over $F[x_1, \ldots, x_n]$ forms a basis for $\mathrm{Map}(\{0,1\}^m, F)$.

Proof. First of all, it is clear that any vector, $\mathbf{x}$, which is nonzero will yield an indicie j, $1 \leq j \leq m$, such that $x_j = 1$ yielding $h(\mathbf{x}) = 0$. So, h is the characteristic function. Now, we prove the set of all monomials forms a basis for $\mathrm{Map}(\{0,1\}^m, F)$.

Recall $|\mathscr{P}([1,m])| = 2^m$ where $\mathscr{P}(X)$ denotes the power set of X. Thus, enumerate all possible subsets of $[1,m]$ as $J_0, J_1, \ldots, J_{2^m-1}$ where $J_0 = \varnothing$ and the rest of the J_i, $1 \leq i \leq 2^m - 1$ are assumed nonempty and ordered by cardinality (so singletons

first, followed by 2-tuples and so on). Next denote all possible monomials

$h_1, \ldots, h_{2^{m-1}} \in F[x_1, \ldots, x_n]$ such that $h_k = \prod_{i \in J_k} x_i$ for each $0 \leq k \leq m$. $\square$

REFERENCES

[1] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[2] George Andrews. *Proc. Advanced Sem., Math. Res. Center, Univ. Wisconsin, Madison, Wis., 1975*.

[3] I. J. Good. Short proof of a conjecture by dyson. *Journal of Mathematical Physics*, 11(6):1884–1884, 1970.

[4] David J. Grynkiewicz. *The Polynomial Method: The Erdos:Heilbronn Conjecture*, volume 30. Springer, 2013.

[5] Gyula Károlyi and Zoltán Nagy. A simple proof of the zeilberger–bressoud q-dyson theorem. *Proceedings of the American Mathematical Society*, 142(9):3007–3011, Sep 2014.

[6] Madan Lal Mehta and Freeman J. Dyson. Statistical theory of the energy levels of complex systems. v. *Journal of Mathematical Physics*, 4(5):713–719, 1963.

[7] Christian Reiher. Reiher, c. on kemnitz' conjecture concerning lattice-points in the plane. *The Ramanujan Journal*, 13, Jun 2007.

[8] Kenneth G. Wilson. Proof of a conjecture by dyson. *Journal of Mathematical Physics*, 3(5):1040–1043, 1962.